REMARKS

Applicants thank the Examiner for the careful and thorough examination of the present application. The Examiner is also thanked for the courtesies extended during the telephonic interview of November 24, 2008, during which the current claim rejections and the prior art were discussed. The patentability of the claims is discussed below.

I. The Claims Are Patentable

The Examiner rejected independent Claims 1, 12, 21, 26 and 36, based on a combination of Dellmo et al., Dichter, and Mitsuoka et al. Independent Claim 12 was rejected further in view of Stevens. Dellmo et al. is directed to a secure wireless LAN device including a housing, a wireless transceiver carried by the housing, and a cryptography circuit carried by the housing. A media access controller (MAC) is included and implements a predetermined wireless LAN MAC protocol. The cryptography circuit includes a cryptography processor, and a control gateway circuit connected to the MAC and the wireless transceiver. The secure wireless LAN device also includes a user network interface carried by the housing and connected to the MAC.

The Examiner correctly recognized that Dellmo et al. does not disclose the user network interface comprising a plurality of different connectors for coupling the cryptographic

module to different network devices. The Examiner also correctly recognized that Dellmo et al. fails to disclose the host network processor generating cryptographic processor command packets for the cryptographic processor each having an address portion and a data portion, and encapsulating command packets for the communications module interface in the data portions of the cryptographic processor command packets. Still further, the Examiner correctly recognized that Dellmo et al. fails to disclose the cryptographic processor passing the communications module command packets to the communications module without performing cryptographic processing thereon.

The Examiner then turned to Dichter for the critical deficiency of the user network interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices. Dichter is directed to a computer network including a plurality of nodes. A programmable switching network allows the nodes to be connected in a plurality of different ways, for example, to selectively allow a node to be connected either as a pass through node or a non-pass through node, and to connect nodes to one another via telephone lines.

The Examiner correctly recognized that even a selective combination of Dellmo et al. and Dichter fails to disclose the host network processor generating cryptographic processor command packets for the cryptographic processor each having an address portion and a data portion, and encapsulating command packets for the communications module interface in the

data portions of the cryptographic processor command packets, and the cryptographic processor passing the communications module command packets to the communications module without performing cryptographic processing thereon. The Examiner turned to Mitsuoka et al. for these critical deficiencies.

Mitsuoka et al. is directed to an access control apparatus and method. More particularly, Mitsuoka et al. discloses controlling accesses to a communications network, the accesses received being based on the iSCSI protocol. A host apparatus outputs a command from its SCSI application layer. The command corresponds to a command frame including both a command and data. Upon reaching and being output from other protocol layers, the command frame is encapsulated in an information frame wherein a SCSI command packet is enclosed by an iSCSIPDU unit, a TCP packet, an IP packet, and an Ethernet head packet.

Applicants respectfully submit that Mitsuoka et al. fails to disclose cryptographic processor command packets for the cryptographic processor each having an address portion and a data portion, and encapsulating command packets for the communications module interface in the data portions of the cryptographic processor command packets. More particularly, the Examiner contended that Mitsuoka et al. discloses "said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion and a data portion, and encapsulating the

command packets (i.e. SCSI CMD/Data) for said communication module in the data portions of a communications module command packet (see Figure 6A, 6B)."

Indeed, if the Examiner contends that the SCSI CMD/Data packet of Mitsuoka et al., Figure 6A, corresponds to the claimed cryptographic processor command packets, each including an address portion and a data portion, then command packets for the communications module are not encapsulated in the data portions of the cryptographic processor command packets, as recited in the independent claims. In other words, Mitsuoka et al. fails to teach encapsulating command packets for the communications module in the data portions of the cryptographic processor command packets. There is nothing in Mitsuoka et al. that teaches or suggests command packets for the communications module encapsulated in the data portions of the SCSI CMD/Data packet.

Alternatively, if the Examiner contends that the information frame illustrated in Figure 6B corresponds to the claimed cryptographic processor command packets, each including an address portion and a data portion, then Mitsuoka et al. fails again to disclose command packets for the communications module are not encapsulated in the data portions of the cryptographic processor command packets, as recited in the independent claims. Instead, Mitsuoka et al. discloses a command, as illustrated in Figure 6A, that "corresponds to a

command frame containing both a command and data." (See Mitsuoka et al., Col. 14, lines 50-52).

Moreover, the iSCSI PDU unit that encapsulates the SCSI CMD/DATA packet includes merely address information, for example, a logical unit number (LUN) and a command descriptor block (COB). Thus, the SCSI command/data packet is encapsulated in address information, and not in the data portions of the cryptographic processor command packets. There is nothing in Mitsuoka et al. that teaches or suggests that the Figure 6A command is encapsulated in a data portion of a cryptographic processor command packet. Indeed, Mitsuoka et al. teaches that the information frame of Figure 6B includes address information.

Additionally, even if Mitsuoka et al. somehow could be interpreted so that the IP packet and TCP packet of Figure 6B, for example, include data portions, Mitsuoka is silent as to what portions of the respective packets the command would be located. Accordingly, the independent claims are patentable for at least this reason alone.

As previously noted, Dellmo et al. is directed to a secure wireless LAN device. A MAC is included and implements a predetermined wireless LAN MAC protocol. The cryptography circuit includes a cryptography processor, and a control gateway circuit connected to the MAC and the wireless transceiver. The secure wireless LAN device also includes a user network interface connected to the MAC.

In contrast, Mitsuoka et al. is directed to a storage control apparatus for controlling an access to a communications network in accordance with the iSCSI protocol, and wherein the access is received via the communications network. (See Mitsuoka et al., Col. 1, lines 1-19; Col. 1, line 64 - Col. 2, line 5). Indeed, Mitsuoka et al. is not related to cryptography. A person having ordinary skill in the art would not turn to the iSCSI protocol communications network access system disclosed in Mitsuoka et al. to generate, process, and pass packets from the internal processors and modules on an ESP independent cryptographic device in Dellmo et al. Accordingly, the combination of Dellmo et al. and Mitsuoka et al. is improper.

Moreover, in Mitsuoka et al., the resulting information frame, as illustrated in Figure 6B, includes the command and/or data encapsulated in a TCP packet, an IP packet, and Ethernet header packet. (See Mitsuoka et al., Col. 14, lines 49-67). For example, the IP packet, and Ethernet header packet includes a target IP address and target host information for a target host or switching device. (See Mitsuoka et al., Col. 12, lines 47-56, and Col. 15, lines 54-59). Implementing Mitsuoka et al. into Dellmo et al. would destroy the functionality of Dellmo et al. since the packets in Dellmo et al. are generated for passing between the cryptographic processor and the communications module internal to the device, not for controlling access to the communications network from an external apparatus. (See Mitsuoka et al., Col. 1, lines 14-18).

Additionally, Applicants respectfully submit that the Examiner's combination of Dellmo et al., Dichter, and Mitsuoka et al. is improper. Applicants point out that Dellmo et al., whose primary objective is to provide greater security in a wireless LAN environment, teaches a secure wireless LAN device, including a housing, a wireless transceiver carried by the housing, and a cryptography circuit carried by the housing. Conversely, Dichter discloses a configurable network that provides a specification compliant topology without requiring the rewiring of a building. A person having ordinary skill in the art would not turn to the programmably configurable computer network of Dichter to combine with the cryptographic device of Dellmo et al.

Still further, Dichter is directed to a wired computer network. As noted above, the wired configurable network of Dichter advantageously allows the use of existing wiring in a building, mainly existing telephone lines. In stark contrast, Dellmo et al. discloses a secure wireless network device. A person having ordinary skill in the art would not combine the wired network of Dichter with the secure wireless network device of Dellmo et al., as not only does Dichter teach away from Dellmo et al, but combining the wired network of Dichter with the secure wireless device of Dellmo et al. would destroy the operability of the Dellmo et al. secure wireless device.

Moreover, one having ordinary skill in the art would not turn to Mitsuoka et al., which is directed to the case where

an external apparatus wishes to access the communications network, to combine with the configurable computer network teachings of Dichter. Accordingly, the Examiner's combination of references is improper.

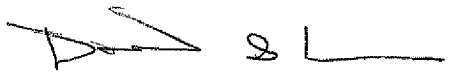
The Examiner also rejected independent Claim 12 over a four-way combination of Dellmo et al., Dichter, Mitsuoka et al., and Stevens. Stevens is cited as disclosing an SNMP protocol. Stevens adds nothing to the critical deficiencies of Dellmo et al., Dichter, and Mitsuoka et al.

Accordingly, it is submitted that the independent claims are patentable over the prior art. In view of the patentability of the independent claims, it is submitted that their dependent claims, which recite yet further distinguishing features, are also patentable over the cited references for at least the reasons set forth above. Accordingly, these dependent claims require no further discussion herein.

II. CONCLUSION

It is submitted that all of the claims are patentable. Accordingly, a Notice of Allowance is therefore respectfully requested in due course. If the Examiner determines any remaining informalities exist, he is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



DAVID S. CARUS
Reg. No. 59,291
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Applicants